UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/886,147	06/20/2001	Kristin E. Lauter	MS1-602US	5710

22801 7590 03/21/2005

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
KIM, JUNG W	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 03/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/886,147	LAUTER ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-47 are pending and have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1-12 and 14-47 are rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for converting the number to an element of the Jacobian of a curve by determining a value a(x), wherein the value a(x) is a monic irreducible polynomial of degree g; determining a value b(x), wherein the value b(x) is a square root of f(x) modulo a(x) of degree less than a(x); and using, as the element of the Jacobian of the curve, the values a(x) and b(x), wherein the conversion is based on an order of a group of points on the Jacobian of the curve, and wherein the order of the group of points on the Jacobian of the curve is maintained as a secret, and wherein the curve is given by the equation y^2=f(x), wherein f(x) has a degree of 2g + 1, and wherein g refers to the genus of the curve, and the corresponding inverse conversion (see specification, pgs. 13-14 and 18-19), does not reasonably provide enablement for converting the number to an element of the Jacobian of the curve (see claim 1) and raising the decompressed value to a particular exponent to obtain a resulting value, wherein the raising is based at least in part on an element of a Jacobian of a curve (see

claim 14). The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the invention commensurate in scope with these claims. The limitation "converting the number to an element of the Jacobian of the curve" covers a much broader spectrum of conversion techniques (including all elliptic curve methods) that is not enabled by the instant specification.

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 39 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 39 recites the limitation "the product identifier" in line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 20-47 are rejected under 35 U.S.C. 101 as not being tangible. None of the recited steps define the use of hardware (ex. processor) to accomplish the steps. Further, the language of claims 20-39 raises a question as to whether the claim is

directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 28, 30, 31, 34, 35, 40, 43, 45 and 46 are rejected under 35 U.S.C. 102(b) as being anticipated by Koblitz Algebraic Aspects of Cryptography (hereinafter Koblitz).

10. As per claims 28, 30, 31, 34, 35, 40, 43, 45 and 46, Koblitz discloses an encryption method and system comprising encrypting a message using a secret, wherein the secret comprises the order of a group of points on the Jacobian, wherein the encrypting comprises receiving the message; wherein the Jacobian comprises a Jocobian of a hyperelliptic curve, wherein the secret comprises the order of a group of points on the Jacobian of a curve, wherein the curve is given by the equation y^2=f(x), wherein f(x) has a degree of 2g + 1, and wherein g refers to the genus of the curve; and a corresponding decryption method and system comprising decrypting a message using a secret, and wherein the secret comprises the order of a group of points on a Jacobian of a curve, wherein the curve comprises a hyperelliptic curve. See Koblitz, pgs. 148-

153, 'Hyperelliptic Cryptosystems', especially section 6.2, 'Example over a Large Prime Field'. The aforementioned covers the limitations of claims 28, 30, 31, 34, 35, 40, 43, 45 and 46.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

13. Claims 1-27 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koblitz in view of Schneier Applied Cryptography (hereinafter Schneier) and Blumenau et al. U.S. Patent No. 6,845,395 (hereinafter Blumenau).

14. As per claims 1, 2 and 5-13, Koblitz discloses a discrete log cryptosystem, wherein a value is converted into an element of the Jacobian of a curve, raising the element to a particular power, and this conversion is based at least in part on an order of a group of points on the Jacobian of the curve, wherein the curve comprises a hyperelliptic curve, wherein the curve is given by the equation of y^2=f(x), wherein f(x) has a degree of 2g + 1, and wherein g refers to the genus of the curve and wherein the order of the group of points on the Jacobian of the curve is maintained as a secret; which further covers the step of converting the number to an element of the Jacobian of a curve comprising determining a value a(z), wherein the value a(x) is a monic irreducible polynomial of degree g; determining a value b(x), wherein the value b(x) is a square root of f(x) modulo a(x) of degree less than a(x); and using as the element of the Jacobian of the curve, the values a(x) and b(x). See Koblitz, pgs. 148-153, 'Hyperelliptic Cryptosystems', especially section 6.2, 'Example over a Large Prime Field'. This conversion has the property of masking the original value of a received value.

15. Koblitz does not expressly teach taking a received value, padding the received value using a recognizable pattern, converting the padded value to a number using a recognizable pattern, wherein converting the padded value to a number represented by a particular number of bits comprises defining a plurality of functions, wherein each of the plurality of functions returns a value that is a set of bits of a hash value generated based on an input value; further, separating the padded value into a plurality of portions and using the plurality of portions as input values for the plurality of functions, wherein

each of the plurality of functions returns a set of least significant bits of a hash value generated based on the input, wherein the hash value is generated using a secure hashing process, wherein the set of bits includes a number of bits equal to half the particular number of bits, and wherein the separating comprises separating the padded value into two equal portions. Schneier discloses using MD5 and SHA hashing algorithms to distill a condense unique value from an original value, wherein this unique value effectively identifies the original value. Operations of this type enable functions to operate on hashed values rather than the corresponding original and larger values to create values linked to the hashed value and by extension to the original value. Further, received values are typically padded as multiples of a number 2^n prior to hashing. In the case of SHA or MD5, n=9. See Schneier, pgs 442-445, section 18.7, 'Secure Hash Algorithm'. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to hash a received value prior to converting the number to an element of a Jacobian curve since it enables the method to take arbitrary-length values and create a fixed length string for computation, which facilitates more efficient processing. See Schneier, pg. 429, section 18.1, 'Background'.

16. Koblitz does not expressly teach compressing the resulting element and outputting the result. However, it is well known in the art to use compression techniques on data such that the data comprises less information but has the reversible property of being decompressed to the original data. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made to compress the resulting value since compressed data has

desirable properties including encoding data to a set length to further enhance processing value of the data as known to one of ordinary skill.

17. Finally, Koblitz does not teach using the aforementioned steps to generate a product identifier. Blumenau discloses encrypting an identifier to prevent other devices from using the identifier and gaining access to services. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to generate a product identifier using the steps taught by Koblitz since product identifiers need to be secured to prevent other devices from using the identifier and gaining access to services. See Blumenau, col. 11:55-61. The aforementioned cover the limitations of claims 1, 2 and 5-13.

18. As per claim 3, the rejections of claims 1, 2 and 5-13 are incorporated herein. Although Koblitz and Schneier only teach padding the received value with zeros, any padding comprising a pattern such that the hash value can be replicated to verify the integrity of a hash is an obvious variation-the portion of the received value is readily available as a padding value. Further, it is notoriously well known to extend the value of a message with any regular pattern up to a fixed multiple as required by methods that process data in blocks. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for the recognizable pattern to comprise at least a portion of the received value, since the received value is readily available as known to one of ordinary skill in the art.

19. As per claim 4, the rejection of claim 1 is incorporated herein. Koblitz does not teach converting the padded value to a 114-bit number. However, the conversion of a value padded to a specific length is typically consistent with the architecture of the underlying process or machine. For example, values output from one step and input to another step require length conversions such that the output value meets the required sized of the input. Hence, the conversion of the padded value to a 114 bit number is a matter of design choice. It would be obvious to one of ordinary skill in the art at the time the invention was made, wherein the padded value is converted to a 114 bit number since the size of the number is dependent on the required size of an input value of a function as known to one of ordinary skill in the art.

20. As per claims 14-27, the rejections of claims 1-13 are incorporated herein. In addition, the encryption method of Koblitz has a corresponding decryption method. Hence, the aforementioned cover the limitations of claims 14-27.

21. As per claim 39, it is a claim corresponding to claims 14-27 and it does not teach or define above the information claimed in claims 14-27. Therefore, claim 39 is rejected as being unpatentable over Koblitz in view of Schneier and Blumenau for the same reasons set forth in the rejections of claims 17-27.

22. Claim 29, 38, 44 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koblitz in view of Schneier.

23. As per claim 29, the rejection of claim 28 is incorporated herein. Koblitz does not expressly teach taking a received value; padding the received value using a recognizable pattern; and converting the padded value to a number represented by a particular number of bits. Schneier discloses using MD5 and SHA hashing algorithms to distill a condense unique value from an original value, wherein this unique value effectively identifies the original value. Operations of this type enable functions to operate on hashed values rather than the corresponding original and larger values to create values linked to the hashed value and by extension to the original value. Further, received values are typically padded as multiples of a number 2^n prior to hashing. In the case of SHA or MD5, n=9. See Schneier, pgs 442-445, section 18.7, 'Secure Hash Algorithm'. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to hash a received value prior to converting the number to an element of a Jacobian curve since it enables the method to take arbitrary-length values and create a fixed length string for computation, which facilitates more efficient processing. See Schneier, pg. 429, section 18.1, 'Background'.

24. Moreover, Koblitz does not expressly teach compressing the resulting element and outputting the result. However, it is well known in the art to use compression techniques on data, such that the data comprises less information but has the reversible property of being decompressed to the original data. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made to compress the resulting value since compressed data has

desirable properties including encoding data to a set length as known to one of ordinary skill. The aforementioned cover the limitations of claim 29.

25. As per claim 38, the rejection of claim 29 is incorporated herein. In addition, the encryption method of Koblitz has a corresponding decryption method. Hence, the aforementioned cover the limitations of claim 38.

26. As per claims 44 and 47, they are claims corresponding to claims 29 and 38 and they do not teach or define above the information claimed in claims 29 and 38. Therefore, claims 44 and 47 are rejected as being unpatentable over Koblitz in view of Schneier for the same reasons set forth in the rejections of claims 29 and 38.

27. Claims 32, 33, 36 and 37 rejected under 35 U.S.C. 103(a) as being unpatentable over Koblitz in view of Blumenau.

28. As per claims 32 and 33, the rejection of claim 28 is incorporated herein. Koblitz does not teach using the encryption method to generate a product identifier. Blumenau discloses encrypting an identifier to prevent other devices from using the identifier and gaining access to services. It would be obvious to one of ordinary skill in the art at the time the invention was made to generate a product identifier using the steps of Koblitz since product identifiers need to be secured to prevent other devices from using the

identifier and gaining access to services. See Blumenau, col. 11:55-61. The aforementioned cover the limitations of claims 32-33.

29. As per claims 36 and 37, the rejections of claims 32-34 are incorporated herein. In addition, the encryption method of Koblitz has a corresponding decryption method. Hence, the aforementioned cover the limitations of claims 36 and 37.

30. Claims 41 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koblitz.

31. As per claims 41 and 42, the rejection of claim 40 is incorporated herein. In addition, Koblitz discloses selecting the curve and the Jocobian of the curve base wherein the parameters include the genus of the curve and the order of the Jacobian of the curve. Ibid. Although Koblitz does not expressly teach a selection module to adaptably change or set the parameters of the encrypting system, means to make adjustable have been found to be obvious enhancement. See In re Stevens 101 USPQ 284 (CCPA 1954). It would be obvious to one of ordinary skill in the art at the time the invention was made for the system of Koblitz to comprise a curve selection module, since it enables a more flexible and secure system by adaptably selecting the parameters to modify the encryption scheme as known to one of ordinary skill in the art.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
March 14, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100